IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Mire, Philip J.	§	
	§	Confirmation No.: 2203
Serial No. 09/312,150	§	
	§	Group Art Unit: 2131
Filed: May 14, 1999	§	
	§	Examiner: Moorthy, Aravind K.
For: PUBLIC KEY INFRASTRUCTURE UTILIZING MASTER KEY ENCRYPTION (AS PREVIOUSLY AMENDED)	§	

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop RCE
Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Responsive to the Final Office Action, dated May 9, 2007, and the Advisory Action dated July 5, 2007, please review the previous response and consider the following remarks in connection with the pre-appeal brief request for review. Review of the final rejection is requested for the following reasons:

1. The phrase "a session key randomly generated" is supported and therefore, a rejection of claims 1, 7-12, 18-22 and 30 under 35 U.S.C. 112 is defective.

Claims 1, 7-12, 18-22 and 30 stand rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The rejection is respectfully traversed.

A written description rejection under 35 U.S.C. §112, first paragraph, places a burden on the USPTO to present a *prima facie* case that the rejected matter does not meet the written description requirement. See MPEP 2163.04. "A written description as filed is presumed to be adequate, unless or until *sufficient evidence or reasoning* to the contrary has been presented by the Examiner to rebut the presumption." *Id.* (Citation omitted). "The Examiner, therefore must have a reasonable basis to challenge the adequacy of the written description" and *MUST* present "by a preponderance of evidence why a person skilled in the art would *not* recognize in an applicant's disclosure a description of the invention defined by the claims." *Id.* Emphasis added. It is submitted that the USPTO has failed to present a *prima facie* case under these requirements and the rejection should be withdrawn.

Application page 2, lines 7-17 discloses that cryptographic systems commonly use a given set of numbers or digits known as a cipher "key" that may be *randomly chosen*. Emphasis added. The term "cipher" is commonly used in the art to refer to cryptographic. Thus, the disclosure implies that ANY key used for cryptographic uses (including a key termed a "session key") may be randomly chosen. Randomly chosen numbers are commonly known in the art as being "generated." Page 7, line 2 discloses that "a session key [is] *generated* by the system." Page 11, lines 11-23 discloses that the "second data processing system 204 includes program instructions to *generate* session key 218." In addition, the Examiner concedes on both page 2 and page 3 of the Final Rejection and on page 2 of the Advisory Action that it is common in the art to generate session keys by a random number.

Given that the specification states a cipher may be randomly chosen , given that a session key is a type of cipher key, given that it is commonly known in the art to generate session keys by random number, and given that the present application discloses that the session key 218 is generated, surely a person skilled in the art *would* recognize in the disclosure a description of the invention defined by the claims as required by MPEP 2163.04 described above. Therefore, it is submitted that the written description requirement of 35 U.S.C. §112 is satisfied and withdrawal of this rejection is respectfully requested.

2. Albanese does NOT teach EVERY element of the claims and therefore, a rejection of claims 1, 7, 8, 12, 18, 19, and 30 under 35 U.S.C. 102(e) is defective.

Claims 1, 7-8, 12, 18-19 and 30 stand rejected under 35 U.S.C. 102(e) as being anticipated by Albanese et al (U.S. Patent No. 6,002,768) (Albanese hereinafter). This rejection is defective and should be withdrawn.

Independent claims 1, 12 and 30 all recite, among other things, encrypting the data using the session key and a symmetric encryption routine; encrypting the session key, with a public key of the first user using an asymmetric encryption routine, for storage as a first user key blob; encrypting the session key, with a master public key using the asymmetric encryption routine, for storage as a master key blob.

The USPTO provides in MPEP §2131 that: "[t]o anticipate a claim, the reference must teach every element of the claim."

Therefore, to support the rejections with respect to claims 1, 7, 8, 12, 18, 19 and 30, Albanese **must** contain **all** of the elements in the above-mentioned claims. However, Albanese **does not disclose** encrypting the data using the session key and a symmetric encryption routine; encrypting the session key, with a public key of the first user using an asymmetric

encryption routine, for storage as a first user key blob; encrypting the session key, with a master public key using the asymmetric encryption routine, for storage as a master key blob.

The rejection points to column 9, lines 37-43 of Albanese to support a claim that Albanese discloses the elements of the pending claims. However, this section of Albanese reads,

> [i]f the lecture is a private conference session, then the confirmation message additionally includes $\{K_S\}k_{Sn}$, the session key K_S encrypted with a public key provided by the requester in its registration request. Since only the requester knows the corresponding private key (written as k_{nij}^{-1} in the case of a service provider), only the requester will be able to obtain the session key from the confirmation message.

Thus, there is no disclosure or suggestion of *encrypting* the *data* using the *session key* and a *symmetric* encryption routine; *encrypting* the *session key*, with a *public key* of the first user using an *asymmetric* encryption routine, for storage as a first *user key blob*; *encrypting* the *session key*, with a *master public key* using the *asymmetric* encryption routine, for storage as a *master key blob*, as recited in the pending claims. Emphasis added.

Additionally, this section of Albanese discloses that the "*session key* K_s [is] encrypted with a public key", NOT that the session key is *used* to encrypt other data. Thus, all the elements of the pending claims are NOT found in Albanese. Furthermore, the present Office Action indicates on page 3 that column 6, lines 31-33 of Albanese discloses that "the key for encryption is the same key for decryption" and thus Albanese uses symmetric encryption. However, the pending claims recite using BOTH symmetric and asymmetric encryption routines. During a quick search of Albanese, neither "symmetric", or "asymmetric" were found. Therefore, Albanese could not disclose, teach, or suggest using one type of encryption over the other. However, the pending claims use both symmetric and asymmetric encryption. Thus, ALL the elements of the pending claims are NOT found in Albanese. As a result, the rejections based on 35 U.S.C. §102(e) cannot be supported by Albanese as applied to claims 1, 12, and 30. Thus, claims 1, 12 and 30 are allowable.

The remaining claims depend from respective ones of the independent claims and are allowable as depending from an allowable claim. Therefore, the remaining claims are allowable as depending from an allowable claim and withdrawal of these rejections is respectfully requested.

3. The rejection of claims 9, 10, 20 and 21 under 35 U.S.C. 103(a) is NOT supported by a *prima facie* case of obviousness.

Claims 9, 10, 20 and 21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Albanese as applied to claims 1 and 12 above, and further in view of Dillaway et al (U.S. Patent No. 5,742,756) (Dillaway hereinafter).

Claims 11 and 22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Albanese as applied to claims 1 and 12 above, and further in view of Kruys (U.S. Patent No. 5,555,309) (Kruys hereinafter). These rejections do not apply to the amended claims for at least the following reason:

Claims 9, 10, 11, 20, 21 and 22 are each dependent claims that depend from either independent claim 1 or 12. As shown above, independent claims 1 and 12 are allowable. Thus, these claims are allowable as depending from an allowable independent claim. Therefore, these rejections are defective and should be withdrawn.

In addition to the previous argument, the PTO recognizes in MPEP §2142:

> The Examiner bears the initial burden of factually supporting any prima facie conclusion of obviousness. If the Examiner does not produce a prima facie case, the applicant is under no obligation to submit evidence of nonobviousness.

The Examiner clearly cannot establish a *prima facie* case of obviousness in connection with claims 9, 10, 11, 20, 21 and 22 for the following reasons.

35 U.S.C. §103(a) provides that:

> [a] patent may not be obtained ... if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains ... (emphasis added)

Thus, when evaluating a claim for determining obviousness, all limitations of the claim must be evaluated. However, Albanese, Dillaway and Kruys, alone, or in any combination, do not teach a method for encrypting data as claimed. In addition to the shortcomings of Albanese as set forth above, Dillaway teaches in the cited section (Column 3, lines 24-31) a smart card that only holds a private key. However, the smart card discussed on page 10, lines 10-19 of the present application "contains the user's private keys and any public keys, as well as any other data that may be required by the systems with which smart card 134 is utilized." Kruys teaches in the cited section (column 2, lines 56-67) "*public* and *private* key pairs which *share the same*

key value." However, the plurality of *private* keys and the plurality of *public* keys claimed in claims 11 and 22 and described on pages 6, line 26 – page 7, line 9 and throughout the application do not have the same key value. For example, with regard to the *public* key, the session key is encrypted twice, once using the *user public* key and once using the *master public* key. Thus, if the plurality of *public keys* were of the same value, there would be no benefit of encrypting the data twice. Additionally, with regard to the plurality of *private* keys, the session key is decrypted using the *user private* key for one user and the session key is decrypted using the *master private* key for a different or third party user. Here again, if the plurality of *private* keys had the same value, there would be no benefit to having the plurality of keys. Therefore, the teaching of Dillaway and Kruys, when combined with the shortcomings of Albanese, do not teach the claimed subject matter as a whole. As a result, it is impossible to render the subject matter of claims 9, 10, 11, 20, 21 and 22 as a whole obvious based on any combination of the patents, and the above explicit terms of the statute cannot be met. As a result, the Examiner's burden of factually supporting a *prima facie* case of obviousness clearly cannot be met with respect to claims 9, 10, 11, 20, 21 and 22, and a rejection under 35 U.S.C. §103(a) is not applicable.

Other reasons for the patentability of the pending claims have been previously presented and will be maintained should the filing of an appeal brief become necessary.

Respectfully submitted,

Bart A. Fisher
Registration No. 55,181

Dated: 7-31-2007

HAYNES AND BOONE, LLP
901 Main Street, Suite 3100
Dallas, Texas 75202-3789
Telephone: 512/867-8458
Facsimile: 214/200-0853
ipdocketing@haynesboone.com

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being transmitted to the United States Patent and Trademark Office, via EFS-Web, on the date indicated below:

on July 31, 2007
Date

M. Kim Reyes
Kim Reyes